SaTC: EDU: Secure and Private Artificial Intelligence

Challenge:

- most students are not exposed to security and privacy issues of machine learning systems and countermeasures
- graduates who may develop and deploy AI systems that are not trustworthy .

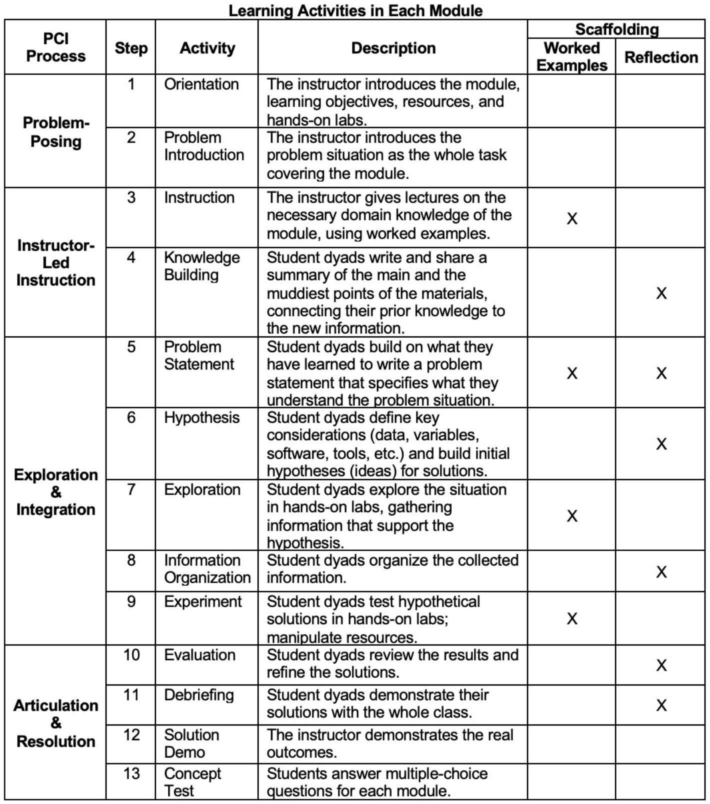
Solution:

- a new course on Private AI to introduce privacy threats, privacy preserving machine learning concepts, techniques, and tools
- utilize best pedagogical practices from the learning sciences, namely principles of problem-centered instruction (PCI)

Award #: 2054968

Georgia State University

PI: Daniel Takabi : takabi@gsu.edu



Learning Activities in Each Module

PCI Process	Step	Activity	Description	Scaffolding	
				Worked Examples	Reflection
Problem-Posing	1	Orientation	The instructor introduces the module, learning objectives, resources, and hands-on labs.		
	2	Problem Introduction	The instructor introduces the problem situation as the whole task covering the module.		
Instructor-Led Instruction	3	Instruction	The instructor gives lectures on the necessary domain knowledge of the module, using worked examples.	X	
	4	Knowledge Building	Student dyads write and share a summary of the main and the muddiest points of the materials, connecting their prior knowledge to the new information.		X
Exploration & Integration	5	Problem Statement	Student dyads build on what they have learned to write a problem statement that specifies what they understand the problem situation.	X	X
	6	Hypothesis	Student dyads define key considerations (data, variables, software, tools, etc.) and build initial hypotheses (ideas) for solutions.		X
	7	Exploration	Student dyads explore the situation in hands-on labs, gathering information that support the hypothesis.	X	
	8	Information Organization	Student dyads organize the collected information.		X
	9	Experiment	Student dyads test hypothetical solutions in hands-on labs; manipulate resources.	X	
Articulation & Resolution	10	Evaluation	Student dyads review the results and refine the solutions.		X
	11	Debriefing	Student dyads demonstrate their solutions with the whole class.		X
	12	Solution Demo	The instructor demonstrates the real outcomes.		
	13	Concept Test	Students answer multiple-choice questions for each module.		

Scientific Impact:

- exposing students to state-of-the-art private AI and preparing them with skills and capabilities for building trustworthy AI systems
- designed and created using the principles of problem-centered instruction (PCI) to build bridges between educational research and subject-matter experts

Broader Impact and Broader Participation:

- impact the competitiveness of the nation by producing trained professionals will help enable the safe adoption of AI systems with privacy protection
- GSU is a minority-serving institution (MSI) + outreach to HBCUs and community colleges in Metro Atlanta